UNITED STATES PATENT AND TRADEMARK OFFICE
DOCUMENT CLASSIFICATION BARCODE SHEET

CATEGORY

CLEARED

ADDRESS
CONTACT IF FOUND:

12-20-99

A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

JC672 U.S. PTO 12/17/99

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 42390.P8081 Total Pages 2

First Named Inventor or Application Identifier Mark A. Beiley

Express Mail Label No. EL034433558US

JC564 U.S. PTO 09/466234 12/17/99

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. X Specification (Total Pages 14)
(preferred arrangement set forth below)
- Descriptive Title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claims
- Abstract of the Disclosure

3. X Drawings(s) (35 USC 113) (Total Sheets 2)

4. X Oath or Declaration (Total Pages 4 (unsigned))
   a. ___ Newly Executed (Original or Copy)
   b. ___ Copy from a Prior Application (37 CFR 1.63(d))
   (for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**
   i. ___ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. ___ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ___ Microfiche Computer Program (Appendix)

7. ___ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ____ Computer Readable Copy
b. ____ Paper Copy (identical to computer copy)
c. ____ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. _____ Assignment Papers (cover sheet & documents(s))
9. _____ a. 37 CFR 3.73(b) Statement (where there is an assignee)
__X__ b. Power of Attorney
10. _____ English Translation Document (if applicable)
11. _____ a. Information Disclosure Statement (IDS)/PTO-1449
_____ b. Copies of IDS Citations
12. _____ Preliminary Amendment
13. __X__ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. _____ a. Small Entity Statement(s)
b. Statement filed in prior application, Status still proper and desired
15. _____ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. _____ Other: _____

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:
___ Continuation ____ Divisional ____ Continuation-in-part (CIP)
of prior application No: _____

18. **Correspondence Address**
_____ Customer Number or Bar Code Label _____
(Insert Customer No. or Attach Bar Code Label here)
or
__X__ Correspondence Address Below

NAME Charles A. Mirho, Registration No. 41,199
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
ADDRESS 12400 Wilshire Boulevard
Seventh Floor
CITY Los Angeles STATE California ZIP CODE 90025-1026
Country U.S.A. TELEPHONE (503) 684-6200 FAX (503) 684-3245
Express Mail Label: EL034433558US

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

METHOD AND APPARATUS TO DETECT CIRCUIT TAMPERING

Inventor: Mark A. Beiley
James E. Breisch

Prepared by: Charles Mirho,
Patent Attorney

intel®
Intel Corporation

"Express Mail" label number EL034433558US

METHOD AND APPARATUS TO DETECT CIRCUIT TAMPERING

BACKGROUND

1. Field

The present invention relates to the detection of tampering with electronic circuits.

2. Background Information

An electronic circuit may be subjected to tampering by third parties attempting to ascertain internal operations of the circuit. For example, the circuit may perform an encryption operation on data using a secret value known as a key. It may be difficult for third parties to ascertain the key value by simply examining the input and output signals to the circuit. By tampering with the circuit, these parties may gain insight into the value of the key employed in the encryption operation.

One form of tampering involves using chemicals or mechanical processes to strip away materials in which the circuits are encased. Such material may include "passivation material", e.g. a form of dielectric or insulator, and may be stripped using chemicals to expose conductive elements of the circuits. Probes may then be placed on the conductive elements to measure signals produced by internal operations of the circuit. The

measurements may allow a third party to ascertain information about the internal operation of the circuit.

SUMMARY

A circuit includes a capacitor formed with a dielectric including the dielectric encasing elements of the circuit. A detector detects changes in the capacitance of the capacitor.

BRIEF DESCRIPTION OF THE DRAWINGS

The subject matter regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, may be further understood by reference to the following detailed description read with reference to the accompanying drawings.

Figure 1 shows an embodiment of a circuit in accordance with the present invention.

Figure 2 shows an embodiment of conductive elements in accordance with the present invention.

Figure 3 shows an embodiment of a tamper detection circuit in accordance with the present invention.

Figure 4 shows an embodiment of voltage signals over time when passivation material is present on and between the conductive elements.

Figure 5 shows an embodiment of voltage over time when passivation material has been stripped from between and/or around the conductive elements.

DETAILED DESCRIPTION

Figure 1 shows an embodiment 100 of a circuit in accordance with the present invention. Embodiment 100 comprises doped regions 110 including doped sub-regions 108. For example, doped regions 110 may be produced using N-type silicon doping and sup-regions 108, also known as "diffusion regions" within regions 110, may be created using P-type silicon doping. Oxide regions 114 may be formed over portions of regions 110 to act as gates. In manners well known in the art, a voltage and/or current signal may be applied to regions 114 to facilitate the exchange of electrons between the regions 108 within a region 110. In other words, regions 110, 114, and 108 may act as a gate-controlled solid state transistor.

A voltage and/or current signal may be provided to regions of the solid state transistors by way of vias 104. Vias 104 act to conduct electrical signals between different layers of circuit 100. Circuit 100 may be organized into layers. Each layer may comprise conductive signal paths 102 for routing electrical signals among various elements of the circuit. Signal paths 102 may be encased within a dielectric material 112, also known as a passivation material or insulator, which protects the signal paths 112 and circuit elements and prevents signals from leaking between various components of the circuit 100. A bonding wire 106 may be coupled to a signal path 102 by way of a via 104 and may conduct signals to and from a terminal of packaging comprising a circuit 100.

Circuit 100 may further comprise conductive elements 116 and 118. Elements 116 and 118 may be arranged approximately parallel to certain signal paths 102 of the circuit 100. Figure 2 shows an embodiment 200 of conductive elements 116 and 118 in accordance with the present invention. Elements 116 and 118 are arranged proximate to one another and approximately parallel. Thus capacitive field 202 may be generated between the elements. A capacitance C resulting from this field 202 may be approximately determined by the following formula:

$$C = (\varepsilon_0 * \varepsilon_R * A)/D$$

Here D is a distance separating facing surfaces of elements 116 and 118 as shown in Figure 2. The symbol A represents the area of the facing surfaces and may be calculated by multiplying the width W of a facing surface by the length L of the facing surface. The

value ε_0 is the well known dielectric constant of a vacuum and has an approximate value of 8.854×10^{-14} F/cm. The value ε_R is the dielectric constant of the material occupying the space surrounding and between the two elements 116 and 118. For example, passivation material 112 may have ε_R of approximately 4, whereas air may have an ε_R value of approximately 1. The formula demonstrates that the capacitance C produced by the approximately parallel arrangement of conductive elements 116 and 118 is directly proportional to the dielectric constant of the material around and between the elements.

Of course, the capacitive field may extend between and around the circuit elements 116 and 118, and thus removal of dielectric material 112 from the vicinity (not just between and immediately around) of the elements 116 and 118 may affect the capacitance C.

Figure 3 shows an embodiment 300 of a tamper detection circuit in accordance with the present invention. Circuit 300 includes two current sources, 302 and 304. In one embodiment, current sources 302 and 304 produce substantially identical, constant current through a range of load conditions. A reference capacitor 308 is provided which is coupled to current source 304. A voltage at node B will increase approximately linearly due to the application of constant current over time to reference capacitor 308. The rate at which the voltage at node B increases is determined by the capacitance of capacitor 308. A second capacitor 306 is coupled to current source 302.

In one embodiment, capacitor 306 is defined by conductive elements 116 and 118. A constant current applied to capacitor 306 by source 302 will increase a voltage at node A approximately linearly over time. The rate at which this voltage increases may be determined by the capacitance of capacitor 306. When either the voltage at node A or the voltage at node B exceeds a predetermined voltage level (logical "high"), OR gate 310 asserts an enable signal to comparator 312. Comparator 312 may be any device which may compare two input signal values to produce an output signal value indicating if one signal has a value less than the other, or alternately if one signal has a value greater than the other. In one embodiment, an output signal 314 of comparator 312 is asserted when the voltage on node A exceeds the voltage on node B. Output 314 is not asserted when the voltage level on node B exceeds the voltage level on node A. Asserted output 314 may be used to disable one or more operations of circuit 100.

Figure 4 shows an embodiment of voltage signals over time on nodes A and B when passivation material 112 is present on and between conductive elements 116 and 118 forming capacitor 306. When passivation material 112 is present, ε_R is approximately equal to a value of 4. This affects the capacitance of capacitor 306 in such a fashion that the voltage on node A increases at a slower rate than the voltage on node B. OR gate 310 asserts an enable signal to comparator 312 when the voltage at B exceeds logical high. At this point in time and thereafter, the voltage at node B exceeds the voltage at node A and the output of comparator 312 is not asserted. Such a condition indicates that passivation material 112 is present between and around the elements of capacitor 306.

Figure 5 shows an embodiment of voltage over time when passivation material 112 has been stripped from between and/or around the elements 116 and 118 of capacitor 306. Note that not all passivation material 112 may be removed. Rather, portions of passivation material 112 may be removed from around and/or between the elements 116 and 118 of capacitor 306. This may occur as a result of physical tampering with circuit 100 in an attempt to access internal components. When the voltage level on node A exceeds logical high, OR gate 310 enables comparator 312. Voltage at node A exceeds the voltage at node B which causes comparator to assert its output signal 314. This condition indicates that passivation material 112 has been removed from around and/or between elements 116 and 118. This condition may indicate tampering. Signal 314 may be employed to disable one or more circuit operations and thus prevent a party responsible for the tampering from obtaining information about internal operations of the circuit.

Elements 116 and 118 may be positioned within circuit 100 such that it may be difficult for a party tampering with the circuit 100 to access important internal components without removing passivation material 112 from around or between elements 116 and 118. Removal of passivation material 112 may result in assertion of tamper detect signal 314, disabling one or more circuit operations.

Once application of the present invention may be found in processor circuits. A computer system may comprise a processor and a memory coupled to the processor by way of a bus. The memory may store instruction signals which, when executed by the

processor, may result in the computer system carrying out certain operations such as reading input signals and producing output signals by way of peripheral devices. The processor may encrypt output signals or decrypt input signals from said peripheral devices. The present invention may be employed to prevent parties from tampering with the processor circuit to determine characteristics of the encryption or decryption operation.

While certain features of the invention have been illustrated as described herein, many modifications, substitutions, changes and equivalents will now occur to those skilled in the art. It is, therefore, to be understood that the appended claims are intended to cover all such embodiments and changes as fall within the true spirit of the invention.

What is claimed is:

1. A circuit comprising:

a capacitor formed with a dielectric including the dielectric encasing elements of the circuit; and

a detector to detect changes in the capacitance of the capacitor.

2. The circuit of claim 1 in which the capacitor further comprises:

approximately parallel conductors located proximate to circuit elements to protect from tampering.

3. The circuit of claim 1 in which the detector further comprises:

a comparator to compare a reference voltage with a voltage at a node of the capacitor.

4. The circuit of claim 1 in which the detector further comprises:

a disable output terminal to provide a signal to disable an operation of the circuit.

5. A circuit comprising:

a detector comprising a capacitor formed from conductive elements arranged such that removal of dielectric material from the vicinity of the conductive elements results in assertion of a signal disabling one or more operations of the circuit.

6. The circuit of claim 5, the detector adapted to assert the signal as a result of a change in a capacitance of the capacitor.

7. The circuit of claim 5, the conductive elements arranged approximately parallel and proximate to elements of the circuit to protect from tampering.

8. The circuit of claim 5, the detector further comprising:

a comparator to compare a reference voltage with a voltage at one of the conductive elements.

9. A method comprising:

disabling one or more operations of a circuit upon detecting a change in a capacitance resulting from removal of dielectric material from the vicinity of conductive elements of the circuit.

10. The method of claim 10 further comprising:

the change in capacitance resulting from removal of dielectric material from the vicinity of approximately parallel conductors located proximate to circuit elements to protect from tampering.

11. The method of claim 11 further comprising:

forming a capacitor using approximately parallel conductors located proximate to circuit elements to protect from tampering; and

comparing a reference voltage with a voltage at a node of the capacitor.

12. A computer system comprising:

a processor coupled to a memory by way of a bus; and

the processor comprising a detector, the detector comprising a capacitor formed from conductive elements arranged such that removal of dielectric material from the vicinity of the conductive elements results in assertion of a signal disabling one or more operations of the circuit.

13. The system of claim 12, the detector adapted to assert the signal as a result of a change in a capacitance of the capacitor.

14. The system of claim 12, the conductive elements arranged approximately parallel and proximate to elements of the processor to protect from tampering.

15. The processor of claim 12, the detector further comprising:

a comparator to compare a reference voltage with a voltage at one of the conductive elements.

ABSTRACT

A circuit includes a capacitor formed with a dielectric including the dielectric encasing elements of the circuit. A detector detects changes in the capacitance of the capacitor.

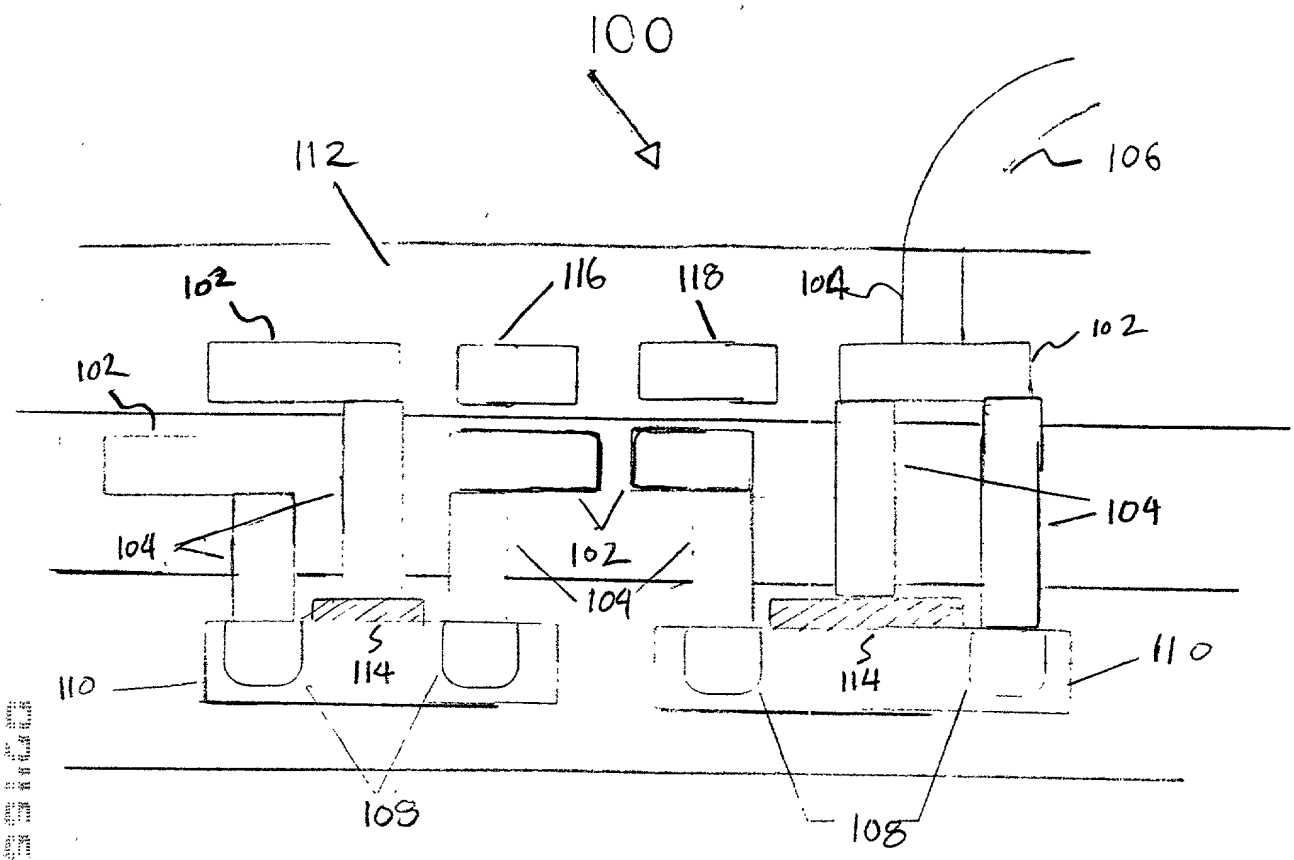
100
112
106
102
116
118
104
102
102
104
102
109
104
114
114
110
110
108
108

FIG. 1

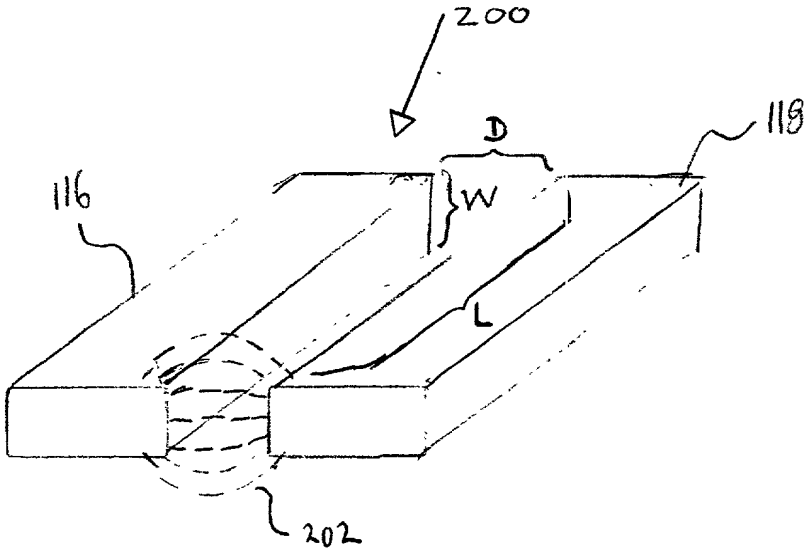
200
D
118
116
W
L
202

FIG. 2

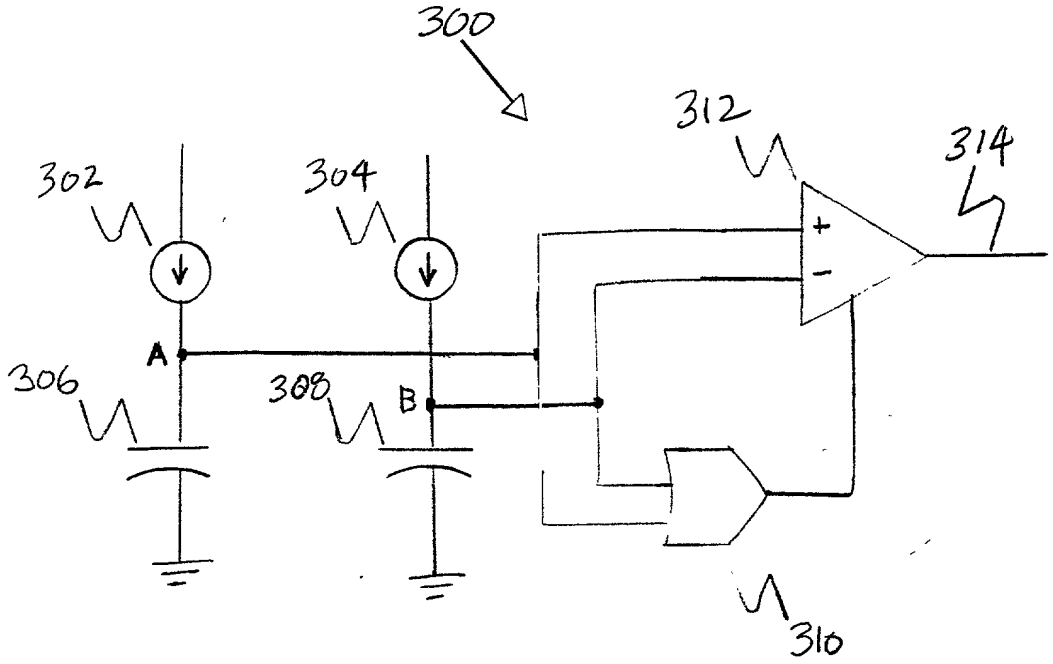

FIG. 3

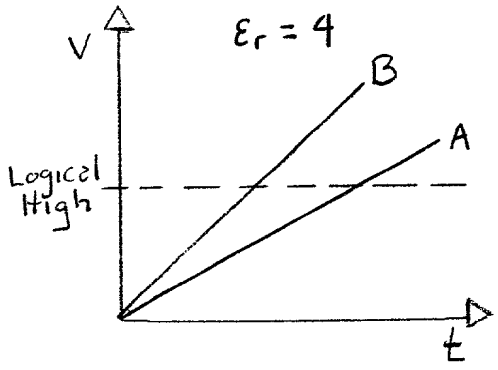

FIG. 4

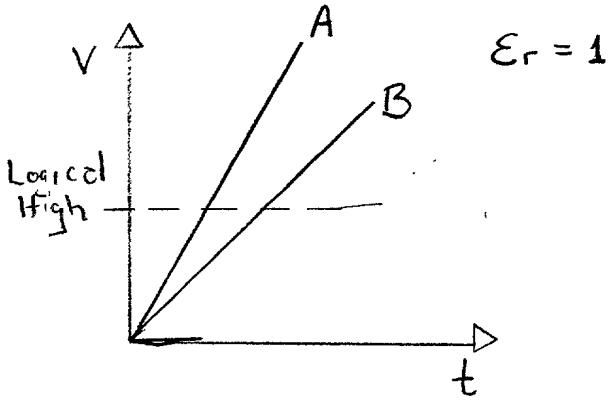

FIG. 5

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR **INTEL CORPORATION** PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD AND APPARATUS TO DETECT CIRCUIT TAMPERING

the specification of which

_XX_ is attached hereto.
____ was filed on _____ as
United States Application Number _____
or PCT International Application Number_____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

(Application Number)	Filing Date
(Application Number)	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number)	Filing Date	(Status -- patented, pending, abandoned)
(Application Number)	Filing Date	(Status -- patented, pending, abandoned)

I hereby appoint Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; Amy M. Armstrong, Reg. No. 42,265; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Kent M. Chen, Reg. No. 39,630; Yong S. Choi, Reg. No. P43,324; Thomas M. Coester, Reg. No. 39,637; Roland B. Cortes, Reg. No. 39,152; Barbara Bokanov Courtney, Reg. No. 42,442; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Tarek N. Fahmi, Reg. No. 41,402; James Y. Go, Reg. No. 40,621; Richard Leon Gregory, Jr., Reg. No. 42,607; Dinu Gruia, Reg. No. P42,996; David R. Halvorson, Reg. No. 33,395; Thomas A. Hassing, Reg. No. 36,159; Phuong-Quan Hoang, Reg. No. 41,839; Willmore F. Holbrow III, Reg. No. P41,845; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; Dag H. Johansen, Reg. No. 36,172; William W. Kidd, Reg. No. 31,772; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Thinh V. Nguyen, Reg. No. 42,034; Kimberley G. Nobles, Reg. No. 38,255; Babak Redjaian, Reg. No. 42,096; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Anand Sethuraman, Reg. No. P43,351; Charles E. Shemwell, Reg. No. 40,171; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; George G. C. Tseng, Reg. No. 41,355; Lester J. Vincent, Reg. No. 31,460; John Patrick Ward, Reg. No. 40,216; Stephen Warhola, Reg. No. 43,237; Charles T. J. Weigell, Steven D. Yates, Reg. No. 42,242; Reg. No. 43,398; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my attorneys, and James A. Henry, Reg. No. 41,064; Daniel E. Ovanezian, Reg. No. 41,236; Glenn E. Von Tersch, Reg. No. 41,364; and Chad R. Walsh, Reg. No. 43,235; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Jeffrey S. Draeger, Reg. No. 41,000; Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells, Reg. No. P43,256; and Alexander Ulysses Witkowski, Reg. No. P43,280; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Charles A. Mirho, Intel Corporation , c/o BLAKELY,
(Name of Attorney or Agent)
SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to
Charles A. Mirho, Intel Corporation , (503)696-8080.
(Name of Attorney or Agent)

INTEL CORPORATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor: Mark A. Beiley

Inventor's Signature: _____ Date: _____

Residence: Chandler, AZ (City, State) Citizenship: USA (Country)

Post Office Address: 1161 N. Dustin Lane, Chandler, AZ 85226

Full Name of Joint/Second Inventor: James E. Breisch

Inventor's Signature: _____ Date: _____

Residence: Chandler, AZ (City, State) Citizenship: USA (Country)

Post Office Address: 1715 W. Morelos St., Chandler, AZ 85224